Microsoft's Enhanced Mitigation Experience Toolkit

A Rationale for Enabling Modern Anti-Exploitation Mitigations in Windows

MIT-001CG-2014
MITIGATIONS GUIDE
OCTOBER 2014

Microsoft®'s Enhanced Mitigation Experience Toolkit (EMET) is an enhancement to the Windows® operating system that stops broad classes of malware from executing. EMET implements a set of anti-exploitation mitigations that prevent the successful exploitation of memory corruption vulnerabilities in software, including many zero-day and buffer overflow attacks. EMET inhibits many of the attacks currently used by Advanced Persistent Threat (APT) actors. EMET is provided by Microsoft at no cost, provides significant software protection for all currently supported versions of the Windows operating system, and supports enterprise deployment and event forwarding (an additional threat analytic source). EMET and its anti-exploitation mitigations are a vital technical component of a cyber defense-in-depth strategy.

Rationale

Leaders, mission managers, and network defenders cannot ignore the cyber threat faced by their organization. Cyber adversaries are exploiting vulnerabilities in legacy systems and un-patched software with greater frequency and detriment. Furthermore, the cost to remediate a network of compromised systems and the cost to recover from the damage to their organization is significant. In response, cyber defenders have invested in detection measures like anti-virus software and blacklists to deter the adversary. These detection measures alone are no longer sufficient. The breadth and complexity of current exploits exceeds many of the protections provided by these reactive defenses.

Organizations should protect their systems with the newest defensive measures and with the most current software. However, the cost to integrate new software and the need for compatibility with legacy applications generally precludes this approach. EMET is a cyber mitigation that addresses cost, integration, and effectiveness:

- EMET is offered at no cost by Microsoft
- EMET provides additional protection to vulnerable un-patched software
- EMET is proven effective against common and targeted exploits
- The principle EMET mitigations are already a part of the Windows operating system, therefore limiting the risk of incompatibilities during integration in the enterprise[1]
- EMET requires little configuration and maintenance after installation

Anti-exploitation mitigations like EMET are increasing in importance. By specifically restricting access to broad classes of exploits, EMET protects software from memory corruption attacks used by many APT actors, protects software in between patch cycles, and protects legacy software even without access to the source code. EMET also integrates with older versions of the Windows operating system, bringing modern anti-exploitation capabilities to these systems. EMET forces the adversary to invent new attack classes from a reduced attack surface, and at a greater cost to them.

1 Although a part of the Windows operating system, the mitigations are not generally enabled. EMET assures that these built-in mitigations are enforced and provides simple management of the mitigations. EMET also introduces additional mitigations not in the operating system for greater security.

Benefits of EMET

As an anti-exploitation mitigation, EMET offers the following benefits:

- **EMET is freely available from Microsoft.**
  Although EMET is provided without cost by Microsoft, an organization must commit some level of trained manpower and resources to configure, test, and install EMET. The DISA Security Technical Implementation Guides (STIGs) define the necessary configuration for system and software settings to offset these costs.

- **Effective cyber mitigation**
  The anti-exploitation mitigations in EMET proactively establish controls within the system to restrict the attack surface (e.g., prohibits data from executing as a program). These controls then inhibit broad classes of attacks, without knowledge of specific exploits or malware specific identifiers. Other defensive systems are reactive, requiring the use of known signatures to identify instances of malware, and require frequent updates as new exploits are discovered. EMET by nature restricts the techniques used for system exploitation without signatures.

- **Does not interfere with legacy and mission critical applications**
  Administrators and cyber defenders can "opt out" their legacy and mission critical applications to ensure that their applications are unaffected by EMET. Furthermore, administrators can load an EMET configuration file that enables various mitigations known to be compatible with commonly-attacked applications.

- **Centralized administration**
  Security mitigations within the operating system are achieved in a patch-work fashion and are not easily enabled for all applications. EMET centralizes the management of these mitigations, adds them to legacy versions of Windows when possible, facilitates their activation, and simplifies their control on each application.

- **Protection during the patch cycle**
  EMET fills the gap between patch cycles, protecting vulnerable software before a patch is developed, and can also protect software that is no longer actively supported and patched.

- **Incremental test and deployment**
  EMET-protected applications can be added incrementally and deployed in an "audit only" mode to monitor application incompatibilities before full deployment.[2]

- **Situational awareness**
  When EMET terminates an application under attack, an event is written to the local event log, which can be collected with Event Log Forwarding. In addition, EMET can be configured to use Windows Error Reporting, which sends alerts to Microsoft or centrally collected in the organization. These alerts can provide early warning of exploit attempts and can bring attention to users or systems that are being attacked.

2 "Audit mode" will report the exploitation attempt and will not terminate the process. This mode is not applicable to all mitigations, since some mitigations are detected when the process is already in a state that cannot be recovered. The mitigations supported by audit mode are: EAF, LoadLib, MemProt, Caller Stack Pivot, Sim Exec FLow, and SEHOP.

Concerns

IT managers and administrators may have concerns including:

- **Windows XP Limitations**
  Although Windows XP does not support two EMET mitigations, Structured Exception Handler Overwrite Protection (SEHOP) and Address Space Layout Randomization (ASLR), EMET provides additional "application specific mitigations" that are beneficial. In fact, EMET is most critical on Windows XP because it provides new protections that never existed in XP, making the operating system less predictable for the attacker.

- **Large Scale Deployment**
  EMET facilitates large scale deployment through Group Policy templates, defining a consistent policy for the organization and managed with the tools already used by administrators.

- **Application Compatibility**
  EMET can be run in an "audit only" mode during testing to reveal any incompatibilities. Thereafter, critical applications can be opted out of EMET protections. EMET provides a list of recommended applications that Microsoft has already tested for compatibility. This is the same list required in DISA's STIGs, and offers excellent protection for commonly-attacked applications. (1)(2)(3)

Technical Background

EMET protects vulnerable software from memory corruption attacks, preventing malware from gaining a foothold within the Windows operating system. The layer of defense provided by EMET inhibits data exfiltration, data theft, and the theft of personally identifiable information (PII) resulting from the installation of malware.

Specifically, EMET provides three (broad) types of mitigations: system wide mitigations, application specific mitigations, and (new in EMET version 4.0) advanced mitigations.[3] These mitigations and the protections they define, represent the overall "attack surface" that EMET defends. The protection defined for each type of mitigation is described below.

System Wide Mitigations

EMET has three system wide mitigations:

- Data Execution Prevention (DEP)
- Address Space Layout Randomization (ASLR)
- Structured Exception Handler Overwrite Protection (SEHOP)

DEP prevents data from executing, and ASLR prevents malware from assembling its malicious activity from (multiple and specific) memory locations by randomizing those locations. SEHOP prevents malware from inserting entries in the structured event handler and executing malicious code referenced by the inserted entry.

An administrator selects a policy for DEP, ASLR, and SEHOP that meets the mission objectives of the organization. For example, an organization can select "opt out," enabling EMET mitigations for all applications, and then exclude any incompatible mission-critical applications.[4] This approach protects the greatest number of applications without impacting critical applications, and is used when risk of exploitation to critical

3 Advanced mitigations also appear in EMET version 5.0. Microsoft released EMET version 5.0 in July 2014, and additionally includes new features, like Attack Surface Reduction (ASR).

4 DISA STIGs require that DEP, ASLR, and SEHOP are set to opt out, opt in, and opt out respectively.

applications is low. Alternatively, an organization may choose "opt in," and then add the commonly targeted applications to the list of EMET-protected applications. "Opt in" would protect the most frequently attacked applications without as much of a risk of incompatibilities.

Application Specific Mitigations

In addition to the system wide mitigations, EMET offers twelve "application specific mitigations" that can be enabled on a per application basis: DEP, SEHOP, NULL Page, Heap Spray, Mandatory ASLR, Export Address Table Access Filtering (EAF), Bottom-up Randomization, Load Library Check, Memory Protection Check, Caller Checks, Simulated Execution Flow, and Stack Pivot.[5] [6]

The specific mitigations are configured by selecting the "Apps" button from EMET's administrative interface (See Figure 1), and by placing a check-mark under a mitigation (See Figure 2). This interface centralizes administration, although simple to use, the interface achieves great effect. As an example, Table 1 depicts two protected applications, and the specific mitigations that are enabled: All twelve mitigations are enabled for the first application, protectedApp_1.exe, and mandatory ASLR is disabled for the second application, protectedApp_2.exe

Application List	DEP	SEHOP	NULL Page	Heap Spray	Mandatory ASLR	EAF	Bottom-Up Randomization	Load Library Check	Memory Protection Checks	Caller Checks	Simulated Execution Flow	Stack Pivot
protectedApp_1.exe	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
protectedApp_2.exe	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓	✓

Table 1 Application Specific Mitigations on a per Application Basis

Advanced Mitigations

EMET version 4.0 introduced three advanced mitigations: Deep Hooks, Anti Detours, and Banned Functions. The advanced mitigations address new and specific exploit code designed to circumvent the system wide mitigations and application specific mitigations. The advanced mitigations are administered from the "Application Configuration" window, in the ribbon, and under "Mitigation Settings" (See Figure 2). These mitigations demonstrate how EMET improves as the threat changes.

5 The DEP, SEHOP, Mandatory ASLR protections under "Application Specific Mitigations" are provided by EMET at the user level, and are not the same as the system wide mitigation of the same name.

6 EMET 5.0 additionally adds EAF+ and Attack Surface Reduction.

Mitigations Reviewed

A list of the system wide mitigations, EMET's advanced mitigations, the application specific mitigations, and the compatible versions of the Windows operating system is shown in Table 2

	Mitigation	XP	Server 2003	Vista	Server 2008	Win7	Server 2008 R2	Win8	Server 2012
System Wide Mitigations	DEP	✓	✓	✓	✓	✓	✓	✓	✓
	ASLR	✗	✗	✓	✓	✓	✓	✓	✓
	SEHOP	✗	✗	✓	✓	✓	✓	✓	✓
Advanced Mitigation	Deep Hooks	✓	✓	✓	✓	✓	✓	✓	✓
	Anti Detours	✓	✓	✓	✓	✓	✓	✓	✓
	Banned Functions	✓	✓	✓	✓	✓	✓	✓	✓
Application Specific Mitigations	DEP	✓	✓	✓	✓	✓	✓	✓	✓
	SEHOP	✓	✓	✓	✓	✓	✓	✓	✓
	NULL Page	✓	✓	✓	✓	✓	✓	✓	✓
	Heap Spray	✓	✓	✓	✓	✓	✓	✓	✓
	Mandatory ASLR	✗	✗	✓	✓	✓	✓	✓	✓
	EAF	✓	✓	✓	✓	✓	✓	✓	✓
	Bottom-up	✓	✓	✓	✓	✓	✓	✓	✓
	Load Library Check	✓	✓	✓	✓	✓	✓	✓	✓
	Memory Protection Check	✓	✓	✓	✓	✓	✓	✓	✓
	Caller Checks	✓	✓	✓	✓	✓	✓	✓	✓
	Simulate Execution Flow	✓	✓	✓	✓	✓	✓	✓	✓
	Stack Pivot	✓	✓	✓	✓	✓	✓	✓	✓

✓ Compatible, ✗ Not compatible

Table 2 EMET Mitigations Available in Windows

Simplified Administration

EMET uses a simple interface to centralize the administration of its mitigations. This interface consists of two windows, the primary EMET window and the "Application Configuration" window (See Figure 1 and Figure 2 respectively).

The primary window, as shown in Figure 1, is titled "Enhanced Mitigation Experience Toolkit", and presents the settings for the system wide mitigations, shows the status of running processes, and presents the "Apps" button.

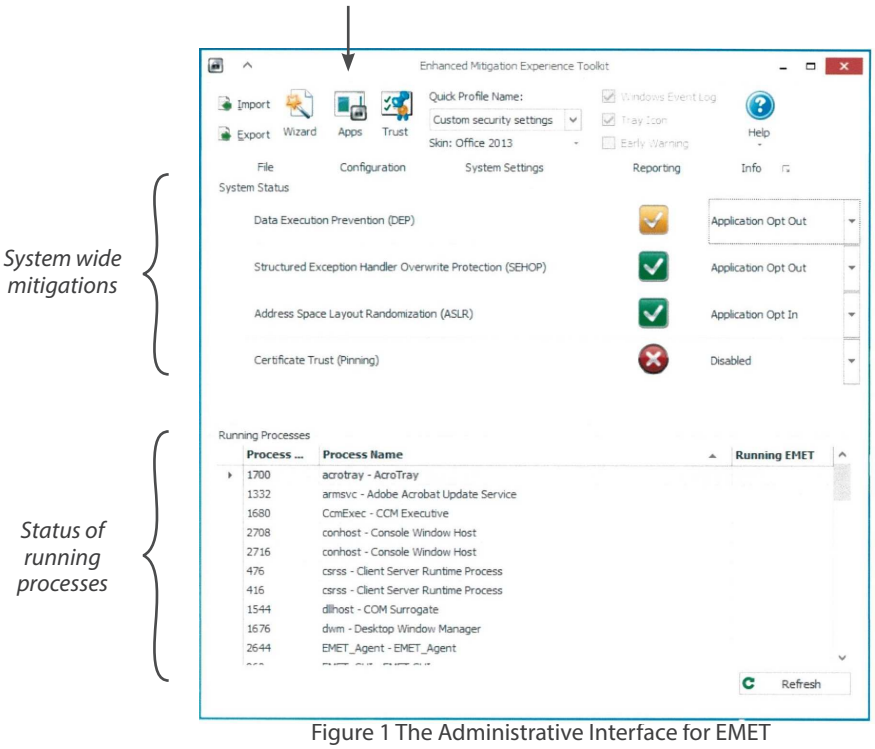

Figure 1 The Administrative Interface for EMET

Figure 2 shows the advanced mitigation settings (Deep Hooks, Anti Detours, and Banned Functions) and the application specific mitigations. The advanced mitigations settings are enabled globally for all applications or are disabled. The application specific mitigations are enabled on a per application basis. For example, a list of applications and the corresponding mitigations are shown in the bottom half of Figure 2. In this instance, all mitigations are applied to each listed application.

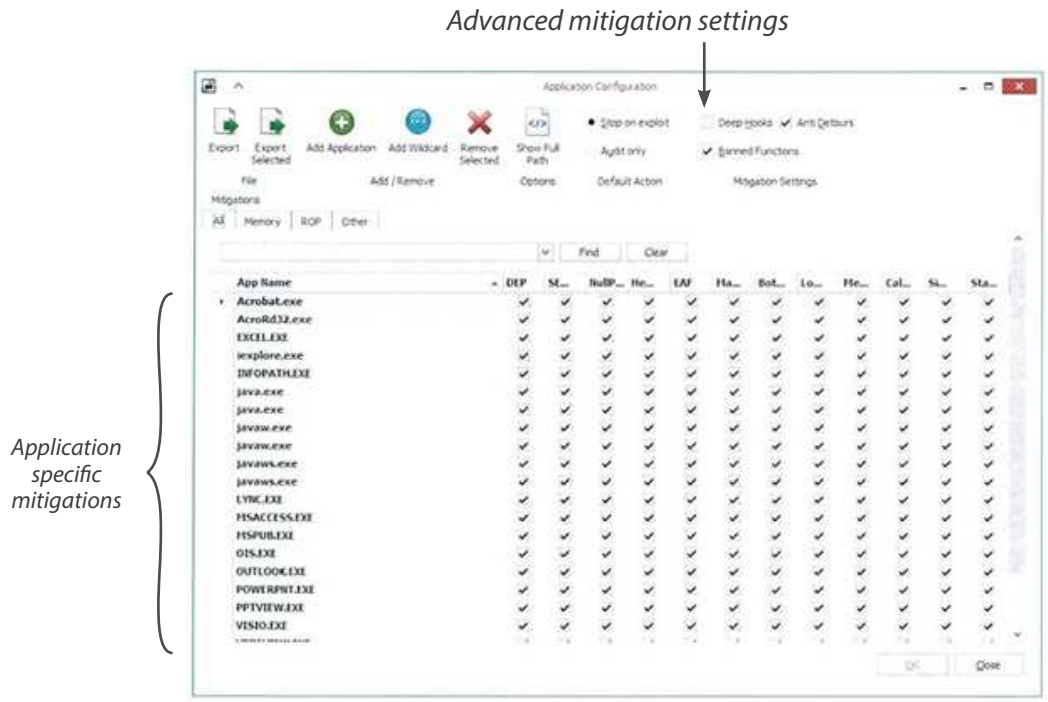

Figure 2 EMET's Application Configuration Window

The application-specific mitigations protect (list) the most commonly attacked applications, exclude individual mitigations that may be incompatible with an application without sacrificing all of EMET's mitigations, and is used such that mission critical applications are precluded.

A Broader View of EMET

EMET is part of a defense-in-depth strategy. As such, EMET has an important role in both the attack lifecycle and within the patch cycle. Namely, EMET is an important mitigation used in the exploitation stage, and a mitigation that reduces risk when a patch is not available.

Disrupting the Attack Lifecycle with EMET

The attack lifecycle presents a model of attacker activity in four broad phases: prepare, get in, stay in, and act. These four phases are then distinguished by activity associated in each phase. For example and during preparation, the attacker establishes policy, conducts reconnaissance, weaponizes their tools, and acquires an infrastructure to stage the attack. During the "get in" phase, the attacker will deliver, exploit the system, and install the malware. The malware then issues a command and control beacon back to the attacker, and in turn this allows the attacker to establish additional persistence mechanisms to stay in the network. After establishing the foothold, the attacker fulfills (acts on) their objective.[7]

7 The model is a generalization and uses broad terminology as a basis for depicting EMET. A specific model would attribute particular threat actors, and would include actions specific to that actor. For example, "goes lateral", "exfiltrates data", or "elevates privileges" would be used in a specific attack model. EMET would still be depicted as a mitigation under the specific model, and under the specific exploit for that model.

A defender uses the model to address the threats to the organization, and defines measures to mitigate threat activities in each phase of the attack. As an example, zero day attacks, buffer overflows, and attacks delivered by malicious websites are common. The organization would then use EMET, an anti-exploitation mitigation, to stop these types of exploits. Figure 3 depicts the attack lifecycle model, shows where the "exploitations" occur, where EMET mitigates the exploit, and shows that attacker access to additional actions in the lifecycle is denied.[8]

Figure 3 EMET Stops the Exploit within the Attack Lifecycle

Although the attack lifecycle in Figure 3 is presented as a sequence, this is a simplification. An attack may repeat or omit certain actions, and even omit entire phases.

EMET in the Software Patch Cycle

When observed in the software patch cycle, EMET reduces the overall security risk of the system.

Namely, an adversary may discover an exploit at any point and deliver that exploit any time prior to the development and installation of the patch. Without EMET, the defender must be aware of these exploits, understand the effect on their system, push appropriate "fixIt" updates to mitigate the vulnerability, and coordinate the installation of the patch when made available. The defender must watch every host. If a compromised host is discovered, the defender must coordinate the triage process and remediate the compromised host. This process within the enterprise is difficult and costly. With EMET, the defender verifies that the system is protected and can install the patch when ready. If an attacker attempts to exploit the vulnerability, EMET will detect and alert the defender to the attack.

8 A complete depiction of attack activities within each phase is omitted for brevity.

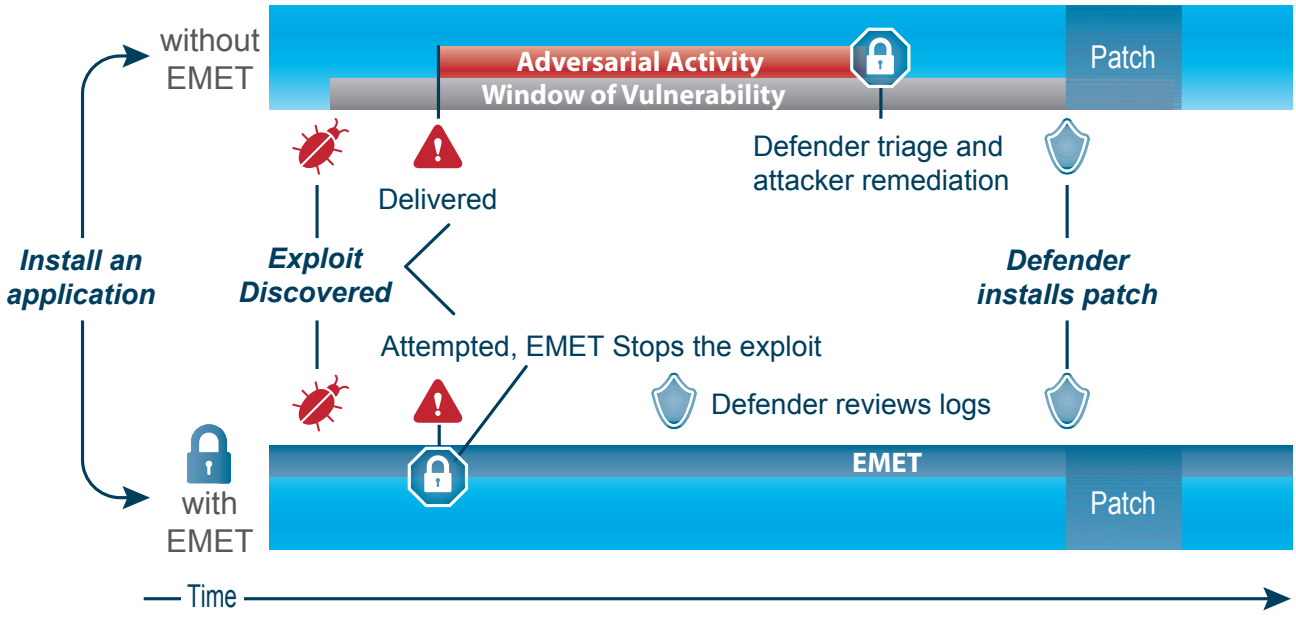

Figure 4 EMET in the Software Patch Cycle

Figure 4 depicts the discovery, exploit, and resulting malicious activity on the system with a vulnerable application, and shows the same application with EMET installed.

Conclusion

EMET is an enhancement to the Windows operating system that stops broad classes of exploits from executing. EMET is provided by Microsoft at no cost, is easy to configure and integrate into the enterprise, and is effective. EMET protects many applications from the attacks commonly used by APT actors. EMET is an anti-exploitation mitigation, is increasing in importance, and provides a vital proactive layer for a defense-in-depth" strategy.

References

1. Windows XP Security Technical Implementation Guide Overview, Version 6, Release 1.29. s.l. : Field Security Operations, Defense Information Systems Agency, 26 Jul 13.

2. Windows 7 Security Technical Implementation Overview, Version 1, Release 12. s.l. : Field Security Operations, Defense Information Systems Agency, 26 Jul 13.

3. Windows 8 Overview, Version 1, Release 2. s.l. : Field Security Operations, Defense Information Systems Agency, 26 Jul 13.

CONTACT INFORMATION

Industry Inquiries
410-854-6091
bao@nsa.gov

USG/IC Customer Inquiries
410-854-4790

DoD/Military/COCOM Customer Inquiries
410-854-4200

General Inquiries
NSA Information Assurance Service Center
niasc@nsa.gov